PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-174445
(43)Date of publication of application : 18.07.1988

(51)Int.Cl. H04L 9/02
G09C 1/00

(21)Application number : 62-006705
(22)Date of filing : 13.01.1987

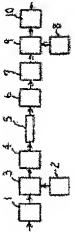
(71)Applicant : NEC CORP
(72)Inventor : YANO MITSUHARU

(54) TRANSMISSION/RECEPTION SYSTEM FOR ENCIPHERED DATA

(57)Abstract:

PURPOSE: To prevent a bit error rate from being deteriorated, by eliminating the distortion of a transmission line by an automatic equalizer, and eliminating the random fluctuation of a transmission symbol position added on a transmission side by a random number group generation circuit.

CONSTITUTION: The position of a transmission symbol from a transmission symbol generator 1 fluctuates at random by the random number group generation circuit 2 and an adder circuit 3, then, it is inputted to a modulation circuit 4. A transmission signal, after receiving the distortion on the transmission line 5, is demodulated at a demodulation circuit 6. The distortion on the transmission line 5 is eliminated at the automatic equalizer 7. Since an authorized receiver can generate one and the same identical random number as that of the transmission side by the random number group generation circuit 8, it is possible to eliminate the fluctuation of the symbol position added on the transmission side by using a subtractor 9. A decision circuit 10 decides the output of the subtraction circuit 9.



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－174445

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和63年(1988)7月18日
H 04 L 9/02		B－7240－5K	
G 09 C 1/00		7368－5B	

審査請求　未請求　発明の数 1　（全4頁）

㊹発明の名称　暗号化データ送受信方式

㉑特　願　昭62－6705
㉒出　願　昭62(1987)1月13日

㉒発 明 者　矢野　光治　東京都港区芝5丁目33番1号　日本電気株式会社内
㉑出 願 人　日本電気株式会社　東京都港区芝5丁目33番1号
㉔代 理 人　弁理士 内原　晋

明　細　書

発明の名称

暗号化データ送受信方式

特許請求の範囲

送信データに応じて送信シンボルを発生する送信シンボル発生回路と、乱数系列を発生する第1乱数系列発生回路と、前記送信シンボル発生回路の出力と前記第1乱数系列発生回路の出力とを加算する加算回路と、前記加算回路の出力を変調し送信信号とする変調回路とを送信側に備え、伝送路を介して受信した前記送信信号を復調する復調回路と、前記復調回路の出力を等化する自動等化回路と、送信側と同一の乱数系列を発生する第2乱数系列発生回路と、前記自動等化回路の出力から前記第2乱数系列発生回路の出力を減算する減算回路と、前記減算回路の出力を判定する判定回路とを受信側に備えることを特徴とする暗号化データ送受信方式。

発明の詳細な説明

〔産業上の利用分野〕

この発明は暗号化データ送受信方式に関する。

〔従来の技術〕

従来、暗号化通信が可能なディジタルデータ伝送方法として送信側では情報源からの2値データ系列をある暗号化アルゴリズムを用いて暗号化された2値データ系列に変換し、変換後の系列を通常の非暗号化データ伝送装置に入力し送信し、受信側では受信信号を通常の非暗号化データ伝送装置に入力し暗号化された2値データ系列を復元し、この系列に送信側で用いた暗号化アルゴリズムの逆変換を施すことにより、情報源にて発生したのと同一の2値データ系列が得られるという方法が知られている。ここで、暗号化アルゴリズムとしては、例えばＤＥＳアルゴリズムが用いられる。

また、別の方法として、送信側では情報源からの2値データ系列を通常の非暗号化データ伝送装置に入力し、得られたアナログ送信信号に対して、

あるアルゴリズムによって得られる別のアナログランダム信号を加算したのち伝送路に送出し、受信側では受信信号から送信側と同一のアナログランダム信号を減算した信号を通常の非暗号化伝送装置に入力することにより、情報源にて発生したのと同一の2値データ系列を得るという方法も加えられている。加算及び減算すべきアナログランダム信号としては、例えば雑音発生器の出力をテープレコーダに録音し、録音されたテープ及びその複製物を送信側及び受信側にて用いることができる。

〔発明が解決しようとする問題点〕

上述の第1の方法においては、通常の非暗号化伝送装置を有する盗聴者は、少なくとも暗号化された2値データ系列は入手することができるので、いったんこの2値データ系列を記録し、その後計算機を用いて、例えば暗号化に用いた鍵をしらみつぶしにあたることにより、これを解読してしまうという危険性が存在する。

また、第2の方法においては、通常の非暗号化

伝送装置を有する盗聴者といえども、アナログランダム信号を減算しない限り、伝送装置は正常に動作しないので2値データ系列自体これを入手することができず、従ってこの方法は第1の方法と比較して解読される危険性が少ないと言える。しかしながら、この方法においては、伝送路において歪みが加わるときには、受信側では送信側で加えたアナログランダム信号そのものではなく、それに歪みが加わった後の信号を減算する必要があり、伝送路の歪みはあらかじめこれを知ることはできないから、この減算を正確に行う事は一般に困難である。従って、その減算の正確さの程度によっては少なくともビット誤り率の劣化、もしくはまったく受信不能といったことが起こりうる。

〔問題点を解決するための手段〕

この発明の暗号化データ送受信方式は送信データに応じて送信シンボルを発生する送信シンボル発生回路と、乱数系列を発生する第1乱数系列発生回路と、前記送信シンボル発生回路の出力と前記第1乱数系列発生回路の出力とを加算する加算

回路と、前記加算回路の出力を変調し送信信号とする変調回路とを送信側に備え、伝送路を介して受信した前記送信信号を復調する復調回路と、前記復調回路の出力を等化する自動等化回路と、送信側と同一の乱数系列を発生する第2乱数系列発生回路と、前記自動等化回路の出力から前記第2乱数系列発生回路の出力を減算する減算回路と、前記減算回路の出力を判定する判定回路とを受信側に備える構成である。

〔実施例〕

以下、本発明を図面に基づいて説明する。

第1図は本発明の基本概念を示す構成図である。第1図において、1は送信側において送信データに応じて送信シンボルを発生する送信シンボル発生回路、2は乱数系列発生回路、3は加算回路、4は変調回路、5は伝送路、6は復調回路、7は自動等化器、8は乱数系列発生回路、9は減算回路、10は判定回路である。

次に、第2図及び第3図を第1図と併用して説明する。ここでは、例として4値AM変調方式が

用いられたものとする。第2図は送信シンボル発生回路1で発生される送信シンボルを示す。送信シンボルの値を3，1，－1，－3とする。送信シンボルは＋1から－1の間の一様乱数を発生する乱数系列発生回路2および加算回路3によって、その位置が第3図に示すようにランダムに変動させられたのち、変調回路4に入力される。送信信号は伝送路5で歪みを受けた後、受信され復調回路6で復調される。伝送路5での歪みは自動等化器7で除去されるので、自動等化器7の出力は加算回路3の出力と等しいものが得られる。正当な受信者は乱数系列発生回路8により送信側と同一の一様乱数を発生させることができるので、減算回路9を用いて送信側で加えた送信シンボルの位置の変動を除去することができる。すなわち、減算回路9の出力として送信シンボル発生回路1の出力と等しいものが得られる。判定回路10はこの減算回路9の出力を判定するのであり、正当な受信者は伝送路5の歪みの存在にもかかわらず、ビット誤り率の劣化をきたすことなく送信データ

を復元することができる。一方、盗聴者は、第３図に示すような自動等化器７の出力までは正当な受信者と同じものが得られるが、送信側と同一の一様乱数を発生させることは少なくともただちにはできないので、第２図に示すような正しく送信シンボルの位置の変動を除去した信号も少なくともただちには得られない。いったん２値データ系列を記録し、その後計算機を用いて、例えば暗号化に用いた鍵をしらみつぶしにあたることにより、これを解読しようと試みても、記録を行う時点では判定回路１０の出力は自動等化器７の出力から乱数の減算を行うことなく、もしくはでたらめな減算を行い、それを判定したものとならざるを得ない。この判定結果が送信データと異なるのはもちろんであるが、さらにこれは判定という非線形操作により既に情報が失われているので、判定回路１０の出力を記録して用いる限り、以後これにいかように操作を施そうとも、送信データを復元することは不可能である。盗聴者が自動等化器７の出力を記録することにより、その後計算機を用

いてこの解読を試みることは一応可能なように思われるが、自動等化器７は一般に判定回路１０の出力を用いてそのタップ係数の更新動作を行うので、判定回路１０の出力が送信データと異なるときには正常な動作は期待できず、従ってこの場合自動等化器７の出力としては加算回路３の出力と同じものすら得られないのでたとえ自動等化器７の出力を記録したとしても、これを用いて送信データを復元することはやはり不可能である。

第４図はこの発明の具体的な構成例を示す。第４図において、１１は２ビットのシフトレジスタ、１２は２ビットかける８ビットのＲＯＭである。ＲＯＭ１２の入出力関係は入力“００”，“０１”，“１０”，“１１”に対して“０１００００００”，“００１００００００”，“１１００００００”，“１１０００００００”がそれぞれ出力されるものとする。２０はＭ系列発生回路、２１は５ビットのシフトレジスタである。３０は８ビットの加算器、４０は８ビットのＤ／Ａ変換器、４１はローパスフィルタ（ＬＰＦ）、４２は正弦波発

生器、４３は乗算器である。５０は伝送路、６０は正弦波発生器、６１は乗算器、６２はローパスフィルタ（ＬＰＦ）、６３は８ビットのＡ／Ｄ変換器、７０は自動等化器、８０はＭ系列発生回路、８１は５ビットのシフトレジスタ、９０は８ビットの減算器、１００は判定器である。

この構成において、２値の送信データはシフトレジスタ１１に入力され、ＲＯＭ１２により４値すなわち６４，３２，－３２，－６４のシンボルの何れかが選択される。Ｍ系列発生回路２０の出力はシフトレジスタ２１により５ビットずつまとめられ、＋３２から－３２の間の一様乱数となる。加算器３０により送信シンボルの位置はランダムに変動されたのち、Ｄ／Ａ変換器４０によりアナログ信号に変換される。この信号はＬＰＦ４１を通過したのち乗算器４３により変調を受け、伝送路５０に送出される。受信側において、受信信号は乗算器６１により復調され、ＬＰＦ６２を通過したのちＡ／Ｄ変換器６３により８ビットのディジタル信号に変換される。この信号は自動等化器７０により伝送路５０の歪みが除去され、送信側と同一のＭ系列発生回路８０により、送信側で加えられた送信シンボルの位置のランダムな変動が減算器９０を用いて除去されるので、判定器１００の出力として送信データが復元される。また、自動等化器７０のタップ係数の更新は判定器１００の出力を用いて通常のグラディエント法により行われる。

〔発明の効果〕

以上説明したように、この発明によれば、通常の非暗号化伝送装置を有する盗聴者にも２値データ系列自体を入手させず、かつ正当な受信者にはビット誤り率の劣化をきたすことのない暗号化データを送受信できる。

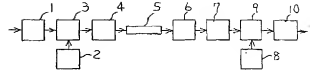
図面の簡単な説明

第１図は本発明の基本概念を示す構成図、第２図及び第３図は本発明の原理を示すためのランダムな位置の変動を受ける前後の送信シンボルを示す図、第４図は本発明の具体的な構成例を示す図

である。

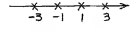
1：送信シンボル発生回路、2，8：乱数系列発生回路、3：加算回路、4：変調回路、5：伝送路、6：復調回路、7：自動等化器、9：減算回路、10：判定回路、11，21，81：シフトレジスタ、12：ROM，20，80：M系列発生回路、30：加算器、40：D／A変換器、43，62：LPF、42，60：正弦波発生器、41，61：乗算器、63：A／D変換器、70：自動等化器、90：減算器、100：判定器。

代理人　弁理士　内原

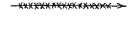


1：送信シンボル発生回路、2,8：乱数系列発生回路、3：加算回路、4：変調回路、5：伝送路、6：復調回路、7：自動等化器、9：減算回路、10：決定回路

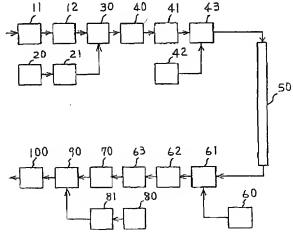
第1図



第2図



第3図



第4図